REMARKS

This is in response to the non-final Office Action mailed November 16, 2007. For at least the reasons stated below, Applicants submit the claims are in condition for allowance and patentable over the prior art of record.

Claims 1, 5 and 8-13 are amended to include additional elements. Generally speaking, these claims are amended to recite the generation and output of either a threat report or a threat presentation. These amendments do not add any new matter beyond the specification, as originally filed, see for example ¶ 0085, which describes the generation and transmission of the threat report 44 and the threat presentation 45. Accordingly, Applicants request entrance and examination.

Claims 1-13 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. While Applicants respectfully disagree, in order to advance the present prosecution, Applicants herein amend the pending claims to include additional limitations of generating either a threat report or a threat presentation and outputting said report or presentation. Therefore, claims 1-13 clearly recite a useful, tangible and concrete result, which includes the generation and output of either the threat report or threat presentation. Applicants request withdrawal of the present rejection.

The Examiner rejects pending claims 5-12 under 35 U.S.C. § 103(a) as being anticipated by U.S. Patent No. 7,089,428 B2 ("Farley") in view of U.S. Published Application No. 2006/0095569 ("O'Sullivan"). Applicants submit this rejection is improper because the combination of Farley and O'Sullivan fails to teach or suggest all of the claimed limitations recited herein.

Farley, as understood, teaches the identification of relationships between attacks on hosts identified by intrusion detection systems and the generation of a correlation event that consists of two sets of lists, inbound attacks relative to the attacked host and outbound attacks relative to the attack host. (see, e.g. col. 12, line 30 - col. 13, line 20). O'Sullivan, as understood, teaches a quality standard monitoring system that observes and analyzes transactions relative to a quality standard. O'Sullivan then generates a trigger in response to the transaction analysis. (see, e.g., ¶ 0018).

Claim 5 recites, *inter alia*, "determining a host threat level based upon a threat weighting assigned to the host associated with a threat weighting assigned to a host network block of which the host is a member." Claim 8 recites, *inter alia*, "determining a source threat based upon a source threat weighting assigned to the source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member." Claims 9-12 recite, *inter alia*, "determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member." Claims 10-12 recite, *inter alia*, "determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member."

Contrary to the Examiner's assertions, O'Sullivan is silent regarding determining any threat value based upon a weighting assigned to the host associated with a weighting assigned to the host associated with a threat weighting assigned "to a host

network block of which the host is a member." The Examiner cites to 5 ¶s in O'Sullivan and Fig. 11, which describe, at best, the weighting of related events "based on each of a user identification associated with the plurality of transactions, transaction identity and an event class associated with the respective ones of the related events to provide weighted related events." (¶ 0029). A further estimation of the Examiner's assertions is possibly the "priority weights" described in ¶ 0090 and Fig. 11, where the prior weights "are applied to events based upon the transaction identity 1102, the user identity 1106 and/or the event class identity 1104." (emphasis added)

The priority weighting of O'Sullivan does not teach or suggest the threat value determination because, among other reasons, O'Sullivan does not include information regarding a "a threat weighting assigned to a host network block of which the host is a member;" (claim 5) "a network block threat weighting for the event type assigned to a host network block of which the host is a member;" (claims 8-12) and "a source threat weighting assigned to a source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member." O'Sullivan's priority weights do not teach or suggest the claimed threat level determinations as asserted on pages 2-10 of the present Office Action.

Accordingly, Applicants submit the rejection is improper and should be withdrawn. In the alternative, Applicants request further clarification as to the exact elements within O'Sullivan that teach or suggest the above-noted claimed limitations.

The Examiner rejects pending claim 1 under 35 U.S.C. § 103(a) as being unpatentable over Farley in view of U.S. Patent No 7,152,105 B2 ("McClure") and further in view of O'Sullivan.

Irrespective of the teachings of Farley and McClure, the Office Action correctly notes that neither Farley or McClure teach or suggest "determining a source threat value, the source threat value based upon a source threat weight for a source IP address and a first range of IP network addresses of which the source IP address is a member;" and "determining a destination vulnerability value, the destination vulnerability value based upon the network event in conjunction with a destination IP address, a destination threat weight for the destination IP address, and a threat level value associated with a second range of network IP address of which the destination IP address is a member."

For brevity's sake, Applicants simply resubmit the above-offered position asserted regarding claims 5-12 that O'Sullivan itself, as well as its priority weights, fails to teach or suggest the claimed limitations. As noted above, O'Sullivan does not teach or suggest weighting values for values on a particular IP address and a range of IP addresses. Accordingly, Applicants submit the rejection is improper and request withdrawal. In the alternative, Applicants request further clarification as to the exact elements within O'Sullivan that teach or suggest the claimed limitation.

Claim 13 stands rejected under 35 U.S.C. §103(a) as being unpatentable over the combination of Farley, McClure and U.S. Published Application No. 2003/0084349 ("Friedrichs").

Irrespective of the teachings of Farley, the Examiner asserts that the claim elements of "determining a first host frequency threat level value by summing event threat level values for a host over a first time period dividing by the number of correlated events for the host in the first time period," "determining a second host frequency threat

level value by summing event threat level values for the host over a second time period greater than the first time period and associated with the number of correlated events for the host in the second time period," "determining a differential threat level denominator by multiplying the second host frequency value by the first time period" and "calculating a differential threat level by dividing the differential threat level numerator by the differential threat level denominator" are disclosed by McClure.

In support of the assertion, the Examiner points to preferred embodiments of McClure for a method of assessing the vulnerability of a target computer via a network (McClure, col. 8, line 59 - col. 9, line 40), a method of creating a topographical representation of a network (McClure, col. 9, line 41 - col. 10, line 16) and a method for calculating an objective security score for a network (McClure, col. 10, lines 15 - 28). The method of assessing the vulnerability of a target computer via a network disclosed in McClure does not contain the claim elements of Independent claim 13. At best, McClure's method of assessing the vulnerability of a target computer via a network includes the step of "calculating an objective indicia of security of the network, the calculation based on a weighted summation of confirmed vulnerabilities." (McClure, col. 9, lines 26 - 28), which is wholly inconsistent with the above-noted elements of claim 13. Applicants additionally note that these positions were previously submitted in the Amendment filed August 27, 2007, to which the Examiner has provided no response.

It is noted that in view of the prior Office Action, the rejection of claim 13 has been updated to include the additional prior art reference of Friedrichs, which is asserted now for teaching the "determining a differential threat level numerator by multiplication of the first host frequency threat level value by the second time period."

Applicants respectfully disagree because ¶ 0037 describes, at best, calculating the frequency of occurrences of a particular security event. A frequency of an event does not teach or suggest the claimed step for determining the differential threat level numerator because a frequency of an event does not teach or suggest the "multiplication" of a "host frequency threat level" by a "time period." Accordingly, Friedrichs fails to teach or suggest the claimed determining of the differential threat level numerator.

Applicants further note that the Examiner asserts McClure of teaching the generation of a denominator value **and** a division operation, but admits that McClure is silent regarding teaching a numerator value used in the division operation. This is an inherent inconsistency that is not addressed in the present office action.

The method for calculating an objective security score for a network disclosed in McClure does not contain the elements of Independent claim 13. At best, McClure discloses a technique wherein "the combination of known vulnerabilities is a summation of weighted numeric expressions if particular vulnerabilities, the weighting based on an ease of exploitation ranking and on access ranking for each vulnerability." (McClure, col. 10, lines 23-28). This is inconsistent with claim 13.

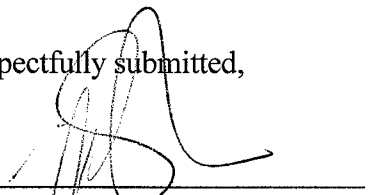
Accordingly, Applicants submit that claim 13 is patentable over the combination of Farley, McClure and Freidrichs for at least the reasons stated above. Applicants request reconsideration and withdrawal. In the alternative, Applicants request further clarification and recitation of support for the exact disclosures of the cited prior art in supporting the present obviousness rejection, including further support regarding the deficiencies Applicants note above.

The Examiner further rejects pending claims 2-4 under 35 U.S.C. § 103(a) as being unpatentable over Farley in view of O'Sullivan in view of McClure and further in view of US Patent No. 6,928,556 B2 to Black, et al. ("Black"). Claims 2-4 depend from claim 1 and recite further patentable subject therefrom. Therefore, claims 2-4 are allowable for at least the same reasons stated above regarding claim 1. Applicants request reconsideration and withdrawal of the present rejection.

For at least all of the above reasons, the Applicants respectfully request that the claims be presented for examination. To expedite prosecution of this application to allowance, the examiner is invited to call the Applicants' undersigned representative to discuss any issues relating to this application.

Dated: February 19, 2008

Respectfully submitted,



THIS CORRESPONDENCE IS BEING SUBMITTED ELECTRONICALLY THROUGH THE PATENT AND TRADEMARK OFFICE EFS FILING SYSTEM ON February 19, 2008.

Jeanpierre J. Giuliano
Reg. No. 55,206
DREIER LLP
499 Park Ave.
New York, New York 10022
Tel : (212) 328-6000
Fax: (212) 328-6001

Customer No. 61834